



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/807,181	06/15/2001	Joerg Schwenk	2345/152	3107

26646 7590 08/26/2004

KENYON & KENYON  
ONE BROADWAY  
NEW YORK, NY 10004

EXAMINER

SON, LINH L D

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 08/26/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/807,181

Applicant(s)

SCHWENK, JOERG

Examiner

Linh Son

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 06/15/2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 4-6 is/are pending in the application.
- 4a) Of the above claim(s) 1-3 is/are withdrawn from consideration. *canceled.*
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 4-6 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 5.
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. This action is responsive to communication: Preliminary Amendment filed on April 9<sup>th</sup> of 2001.
2. For IDS received on April 9<sup>th</sup> of 2001, the IDS fails to comply with 37 CFR 1.98(d), which requires A copy of any patent, publication, pending U.S. application or other information, as specified in paragraph (a) of this section, listed in an information disclosure statement is required to be provided. The Non-patent literatures listed in the PTO-Form 1449 are missing. Examiner requests the applicant to resubmit all the missing Non-patent literatures for consideration.

### ***Claim Rejections - 35 USC § 102***

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 4-5 are rejected under 35 U.S.C. 102(e) as being anticipated by Flat, US Patent No. 5592552, hereinafter '552.

5. As to independent claim 4, ***"A process for establishing a common cryptographic key for  $n$  subscribers using the Dilie-Hellman process"*** is taught in '552 (Col 5 lines 37-45). ***"Comprising: assigning the  $n$  subscribers respective leaves of a binary-structured tree which has a root,  $n$  Leaves, is of depth  $\lceil \log_2 N \rceil$  and has tree-nodes, for each one of the  $n$  subscribers, generating a respective secret, the respective secret being assigned to the one of the  $n$  Leaves to which the one of the  $n$  subscribers is assigned"*** is taught in '552 (Col 12 lines 13-24, lines 39-55, and Figure 3); ***"establishing secrets consecutively in a direction of the root of the tree for all  $k$  nodes of the tree starting from the  $n$  Leaves of the tree across an entire hierarchy of the tree, wherein two already known secrets are combined using the Diffie-Hellman process to form a new common secret, the new common secret being allocated to a common node so that a common cryptographic key for all  $n$  subscribers is allocated to a last one of tree nodes, the last one of the tree nodes being the root of the tree"*** is taught in '552 (Col 12 lines 5-58).

As to dependent claim 5, ***"The process as recited in claim 4, further comprising: adding a new subscriber to the  $n$  subscribers of the tree so that there are  $n+1$  subscribers of the tree, the adding step including: adding two new leaves as successors to a selected one of the  $n$  Leaves of the tree so that the new tree has  $n+1$  Leaves and is of depth  $\lceil \log_2 (n+1) \rceil$  ; assigning the one of the  $n$  subscribers***

***to whom the selected one of the  $n$  Leaves is assigned one of the two new Leaves and assigning the new subscriber to another one of the two new Leaves, the selected one of the  $n$  Leaves becoming a common node for the two new Leaves, and starting from the new Leaves in a direction of the root of the tree, establishing new secrets only in those of the tree nodes which lie within a framework of the tree on a path from the two new Leaves to the root of the tree"*** is taught in '552 (Fig 3, Col 13 lines 54-62, Col 12 lines 39-57, and Col 12 lines 20-24).

### ***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Flat in view of Schwenk, US Patent No. 6222923.

8. As to dependent claim 6, Flat teaches the process as recited in claim 4. However, Flat does not specifically teach the steps of regenerating the common cryptographic key in the event of a subscriber removed from the tree. Nevertheless, Schwenk does teach the method of generating the common cryptographic key can be implemented to create a new key in the event of a subscribers removed from the tree

(Col 3 lines 24-62, and Figure 1 and 2). Therefore, it would also be obvious at the time of the invention was made for one having ordinary skill in the art to implement the method to ensure an updated common cryptographic key.

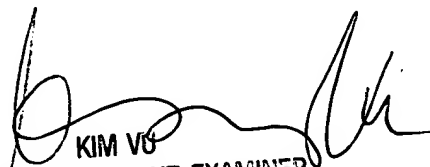
**Conclusion**

9. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (703)-305-8914.

10. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (703)-305-4393. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (703)-305-9600.

**Linh LD Son**

**Patent Examiner**

  
KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100